



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,920	03/30/2004	Timo P. Tervo	944-004.047	5042

4955 7590 05/05/2006

WARE FRESSOLA VAN DER SLUYS &
ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

EXAMINER

WENDELL, ANDREW

ART UNIT PAPER NUMBER

2618

DATE MAILED: 05/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/813,920	Applicant(s) TERVO ET AL.	
	Examiner Andrew Wendell	Art Unit 2618	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 07 April 2006.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10,12-21,24 and 25 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10,12-21,24 and 25 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-7, 10, 12-19, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morriss et al. (US Pat Appl# 2004/0203601) in view of Kokubo (US Pat Appl# 20040224665).

Regarding claim 1, method claim 1 is rejected for the same reason as apparatus claim 13 since the recited elements would perform the claimed steps.

Regarding claim 2, method claim 2 is rejected for the same reason as apparatus claim 14 since the recited elements would perform the claimed steps.

Regarding claim 3, method claim 3 is rejected for the same reason as apparatus claim 15 since the recited elements would perform the claimed steps.

Regarding claim 4, method claim 4 is rejected for the same reason as apparatus claim 16 since the recited elements would perform the claimed steps.

Regarding claim 5, method claim 5 is rejected for the same reason as apparatus claim 17 since the recited elements would perform the claimed steps.

Regarding claim 6, method claim 6 is rejected for the same reason as apparatus claim 18 since the recited elements would perform the claimed steps.

Regarding claim 7, Morriss et al. teaches wherein the user provides the personal identification code to an attendant (wireless service provider), and the attendant then sends the guard message (Section 0011).

Regarding claim 10, it is well know that when uploading can be encrypted in order to protect data from individuals. The examiner takes an official notice to this effect.

Therefore, it would have been obvious at the time of the invention to one of ordinary skill in the art at the time the invention was made to incorporate encrypted data in order to increase security of personal data.

Regarding claim 12, Morriss et al. teaches a computer readable medium encoded with a software data structure (Section 0019).

Regarding claim 13, Morriss et al. apparatus for activating a restrictive operating mode of a wireless communication device teaches a transceiver for receiving a guard message 101 (Fig. 1); an authentication unit for authenticating the guard message and providing an authentication signal (Section 0011); a communication locking mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal (Section 0011), a data securing mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal (Section 0004), wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile terminal (Section 0011). Morriss et al. fails to teach destroying data and uploading the data.

Kokubo's mobile terminal apparatus teaches a transceiver for receiving a guard message 100 (Fig. 1); an authentication unit for authenticating the guard message and providing an authentication signal S601 and S602 (Fig. 6); a communication locking mechanism S605 (Fig. 6), responsive to the authentication signal S602 (Fig. 6); a communication locking mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal S605 (Fig. 6); a data securing mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal S605 (Fig. 6), wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile terminal (Section 0046), and wherein the data securing mechanism is also for destroying S608 (Fig. 6) the at least part of the stored data is accomplished after uploading S606 (Fig. 6) the at least part of the stored data from the mobile terminal.

Therefore, it would have been obvious at the time of the invention to one of ordinary skill in the art at the time the invention was made to incorporate destroying data and uploading the data as taught by Kokubo into Morriss et al. apparatus for activating a restrictive operating mode of a wireless communication device in order to protect the information on the mobile terminal faster (Section 0009).

Regarding claim 14, the combination including Morriss et al. teaches wherein the guard message employs a smart message implemented as a bearer-independent object (wireless messages, section 0054).

Regarding claim 15, the combination including Kokubo teaches wherein the guard message employs synchronization markup language device management (e-mail, sections 0045-0046).

Regarding claim 16, Morriss et al. apparatus for activating a restrictive operating mode of a wireless communication device teaches a transceiver for receiving a guard message 101 (Fig. 1); an authentication unit for authenticating the guard message and providing an authentication signal (Section 0011); a communication locking mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal (Section 0011), a data securing mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal (Section 0004), wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile terminal (Section 0011), and employs a smart message implemented as a bearer-independent object or employs wireless access protocol push messaging (wireless messages, section 0054). Morriss et al. fails to teach destroying data and uploading the data.

Kokubo's mobile terminal apparatus teaches a transceiver for receiving a guard message 100 (Fig. 1); an authentication unit for authenticating the guard message and providing an authentication signal S601 and S602 (Fig. 6); a communication locking mechanism S605 (Fig. 6), responsive to the authentication signal S602 (Fig. 6); a communication locking mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal S605 (Fig. 6); a data securing

mechanism, responsive to the authentication signal, for securing at least some data that is stored in the mobile terminal S605 (Fig. 6), wherein the guard message is transmitted to the transceiver when the user inputs a personal identification code at a location separate from the mobile terminal (Section 0046), and wherein the data securing mechanism is also for destroying S608 (Fig. 6) the at least part of the stored data is accomplished after uploading S606 (Fig. 6) the at least part of the stored data from the mobile terminal, and wherein the guard message employs synchronization markup language device management (e-mail, sections 0045-0046).

Note, it is obvious to combine synchronization markup language (e-mail, using conventional http connection or synchronization) or if the devices don't support synchronization markup language then smart message implemented as a bearer-independent object or employs wireless access protocol push messaging (text messages) since both references teach about each communication type. Kokubo teaches more than one communication mode (e-mail, DTMF signal, and web).

Regarding claim 17, the combination including Morriss et al. teaches wherein the personal identification code (Section 0011 and 0016) is different from a code used to operate the mobile terminal, and wherein transmission of the guard message also requires inputting a mobile terminal identifier (Section 0003). Morriss et al. does not specifically mention about a mobile terminal identifier but the possibility of having that feature could be implemented and obvious.

Therefore, it would have been obvious at the time of the invention to one of ordinary skill in the art at the time the invention was made to incorporate multiple

passwords as taught by Morriss et al. in order to improve security of a lost device (Section 0005).

Regarding claim 18, Morriss et al. teaches the possibility of wherein the personal identification code and the code used to operate the mobile terminal are both user-selected which is obvious (Section 0003, 0011, and 0016).

Regarding claim 19, Morriss et al. teaches wherein the guard message is received from an attendant (wireless service provider), in response to the attendant obtaining the personal identification code from the user (Section 0011).

Regarding claim 25, it is well known that when uploading can be encrypted in order to protect data from individuals. The examiner takes an official notice to this effect.

Therefore, it would have been obvious at the time of the invention to one of ordinary skill in the art at the time the invention was made to incorporate encrypted data in order to increase security of personal data.

3. Claims 8 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morriss et al. (US Pat Appl# 2004/0203601) in view of Kokubo (US Pat Appl# 2004/0224665) as applied to claim 1 and 13 above, and further in view of Isaksson et al. (US Pat# 6,865,232).

Regarding claim 20, Morriss et al. apparatus for activating a restrictive operating mode of a wireless communication device in view of Kokubo's mobile terminal apparatus teaches the limitations in claim 13. Morriss et al. and Kokubo fail to teach about sending a message repeatedly until an acknowledgment is received.

Isaksson et al. multi-carrier transmission system teaches wherein the guard message is sent repeatedly to the transceiver until an acknowledgment is received from the transceiver (Col. 29 lines 17-21).

Therefore, it would have been obvious at the time of the invention to one of ordinary skill in the art at the time the invention was made to incorporate sending a message repeatedly until an acknowledgment is received as taught by Isaksson et al. into destroying data and uploading the data as taught by Morriss et al. in view of Kokubo apparatus for activating a restrictive operating mode of a wireless communication device in order provide better communication (Col. 2 lines 50-53).

Regarding claim 8, method claim 8 is rejected for the same reason as apparatus claim 20 since the recited elements would perform the claimed steps.

4. Claims 9 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Morriss et al. (US Pat Appl# 2004/0203601) in view of Kokubo (US Pat Appl# 2004/0224665) and further in view of Isaksson et al. (US Pat# 6,865,232) as applied to claims 8 and 20 above, and further in view of Helle (EP 1170969).

Regarding claim 21, Morriss et al. in view of Kokubo and further in view of Isaksson et al. teach the limitations in claims 8 and 20. Isaksson et al., Morriss et al., and Kokubo fail to teach information to where the mobile terminal is located.

Helle's apparatus for controlling and securing mobile phones that are lost, stolen or misused teaches wherein the acknowledgment includes information about where the mobile terminal is located (Section 0010).

Therefore, it would have been obvious at the time of the invention to one of ordinary skill in the art at the time the invention was made to incorporate information to where the mobile terminal is located as taught by Helle into sending a message repeatedly until an acknowledgment is received as taught by Isaksson et al. into destroying data and uploading the data as taught by Kokubo into Morriss et al. apparatus for activating a restrictive operating mode of a wireless communication device in order improve security and make it easier to find a phone (Section 0009 and 0016).

Regarding claim 9, method claim 9 is rejected for the same reason as apparatus claim 21 since the recited elements would perform the claimed steps.

5. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Morriss et al. (US Pat Appl# 2004/0203601) in view of Kokubo (US Pat Appl# 2004/0224665) as applied to claim 13 above, and further in view of Ishida (US Pat# 6,212,410).

Regarding claim 24, Morriss et al. apparatus for activating a restrictive operating mode of a wireless communication device in view of Kokubo's mobile terminal apparatus teaches the limitations in claim 13. Morriss et al. and Kokubo fail to teach about an emergency power supply.

Ishida's portable telephone apparatus with security function teaches an emergency power supply 18 (Fig. 1) that could be used for at least powering the communication locking mechanism and the data securing mechanism if normal power 12 (Fig. 1) to the mobile terminal is disabled.

Therefore, it would have been obvious at the time of the invention to one of ordinary skill in the art at the time the invention was made to incorporate an emergency power supply as taught by Ishida into destroying data and uploading the data as taught by Morriss et al. in view of Kokubo apparatus for activating a restrictive operating mode of a wireless communication device in order to secure a portable telephone unit without the need to activate a security function (Col. 1 line 66-Col. 2 line 3).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Hasebe discloses a system for remotely securing/locking a stolen wireless device via an e-mail message. Hayward discloses personal data device and protection system and method for storing and protecting personal data. Tanaka et al. discloses a portable information processing device having data evacuation function and method thereof.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew Wendell whose telephone number is 571-272-0557. The examiner can normally be reached on 7:30-5 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nay Maung can be reached on 571-272-7882. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2618

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Andrew Wendell
Examiner
Art Unit 2618

4/26/06



NAY MAUNG
SUPERVISORY PATENT EXAMINER